IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SPA SYSPATRONIC AG, Plaintiff, v. VERIFONE, INC., VERIFONE HOLDINGS, INC., HYPERCOM CORP., INGENICO CORP., and INGENICO S.A., Defendants.	§	BY Civil Action No. 2:07cv416 LED JURY DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff SPA Syspatronic AG (hereinafter "Syspatronic"), by its counsel, alleges as follows:

NATURE OF THE ACTION

1. This action is for injunctive relief and damages for patent infringement by Defendants VeriFone, Inc., VeriFone Holdings, Inc., Hypercom Corp., Ingenico Corp., and Ingenico S.A. (hereinafter "Defendants") of United States Patent No. 5,093,862 owned by Syspatronic.

THE PARTIES

2. Plaintiff Syspatronic is a corporation of Switzerland, having a principle place of business at Lauriedstrasse 7, CH-6300 ZUG, Switzerland.

3. Defendant VeriFone, Inc. is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 2099 Gateway Place, Suite 600,

San Jose, CA 95110. Defendant VeriFone Holdings, Inc. is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 2099 Gateway Place, Suite 600, San Jose, CA 95110.

4. On information and belief, Defendant Hypercom Corp. is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 2851 W. Kathleen Road, Phoenix, Arizona 85053.

5. Defendant Ingenico Corp. is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 6195 Shiloh Road, Suite D, Alpharetta, GA 30005. Defendant Ingenico S.A. is a corporation of France, having a principle place of business at 192, avenue Charles de Gaulle, 92200 Neuilly-sur-Seine, France.

6. Defendants manufacture, sell, and offer to sell credit card payment modules and terminals in this district and throughout the world.

JURISDICTION AND VENUE

7. This is an action for patent infringement. The claims arise under the patent laws of the United States, Title 35 §§ 1 *et seq.*

8. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

9. On information and belief, Defendants are subject to personal jurisdiction within this district because Defendants have availed themselves to the laws of the state of Texas and conduct business activities in Eastern District of Texas. These business activities include systematically and continuously selling and offering to sell credit card payment modules and terminals throughout the Eastern District of Texas.

10. On information and belief, Defendants regularly direct contacts toward the residents of the Eastern District of Texas. Such contacts include developing a commercial and interactive website available to the residents of the Eastern District of Texas. The website promotes and facilitates the transaction of business between its visitors to the web site and the Defendants.

11. On information and belief, through their acts of infringement, Defendants have harmed the interests of Syspatronic and caused damages in the Eastern District of Texas.

12. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c), and 28 U.S.C. § 1400(b).

THE PATENT IN SUIT

13. United States Patent No. 5,093,862 ("the '862 patent") (attached hereto as Exhibit A), entitled "Data Carrier-Controlled Terminal in a Data Exchange System," was duly and legally issued by the United States Patent and Trademark Office ("USPTO") on July 18, 1989.

14. Syspatronic is the owner by valid assignment of all right, title, and interest in the '862 patent.

COUNT I: INFRINGEMENT OF THE '862 PATENT

15. Syspatronic incorporates by reference each and every allegation set forth in paragraphs 1 through 14 of the Complaint.

16. On information and belief, Defendants VeriFone Holdings, Inc. and VeriFone, Inc have been and are infringing, contributing to the infringement of, and/or inducing the infringement of one or more claims of the '862 patent pursuant to 35 U.S.C. §271 by making, using, selling, and/or offering for sale products and technology covered by the '862 patent

themselves and through their customers. The infringing products include, by way of example, the OMNI 7XXX product family.

17. On information and belief, Defendants VeriFone Holdings, Inc. and VeriFone, Inc have been and are infringing one or more claims of the '862 patent pursuant to 35 U.S.C. §271 by supplying or causing to supply, in or from the United States all or a substantial portion of the components of the '862 patent in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the '862 patent if such a combination occurred within the United States. The infringing products include, by way of example, the OMNI XXXX, Vx(XXX), and SC XXX product families.

18. On information and belief, Defendants VeriFone Holdings, Inc. and VeriFone, Inc have been and are infringing one or more claims of the '862 patent pursuant to 35 U.S.C. §271 by supplying or causing to supply, in or from the United States one or more components of the patented invention that is/are especially made or especially adapted for use in the patented invention and not a staple article or commodity of commerce suitable for substantial noninfringing use, knowing that such component is so made or adapted and intending that such component will be combined outside of the United States in a manner that would infringe the patent if such combination occurred within the United States. The infringing products include, by way of example, the OMNI XXXX, Vx(XXX), and SC XXX product families.

19. On information and belief, and likely to have evidentiary support after a reasonable opportunity for further investigation or discovery, Defendant Hypercom Corp. has been and is infringing, contributing to the infringement of, and/or inducing the infringement of one or more claims of the '862 patent pursuant to 35 U.S.C. §271 by making, using, selling, and/or offering for sale products and technology covered by the '862 patent themselves and

through their customers. The infringing products include, by way of example, the Optimum L4XXX product family.

20. On information and belief, Defendants Ingenico Corp. and Ingenico S.A. have been and are infringing, contributing to the infringement of, and/or inducing the infringement of one or more claims of the '862 patent pursuant to 35 U.S.C. §271 by making, using, selling, and/or offering for sale products and technology covered by the '862 patent themselves and through their customers. The infringing products include, by way of example, e^N Touch 1000 and the i6XXX product families including the contactless expansion module.

21. By reason of Defendants' acts alleged herein, Syspatronic has suffered, is suffering, and will continue to suffer injury to its business and property rights for which it is entitled to damages in an amount to be proved at trial.

22. As a result of Defendants' infringement of the '862 patent, Syspatronic has suffered, is suffering, and will continue to suffer irreparable harm unless such acts are enjoined by the Court.

23. Upon information and belief, Defendants' infringement of the '862 patent was and is willful and with full knowledge of the '862 patent, thereby rendering this case exceptional under 35 U.S.C. § 285 and entitling Syspatronic an award of reasonable attorneys fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff SPA Syspatronic AG respectfully requests the following relief:

A. Judgment that Defendants have infringed, directly or indirectly, one or more claims of the '862 patent and that such infringement has been and is willful;

B. A permanent injunction restraining and enjoining Defendants and their officers, agents, attorneys and employees, and those acting in privity or concert with them, from engaging in further acts of infringement of the '862 patent;

C. An award to Plaintiff SPA Syspatronic AG of all compensatory damages resulting from the direct and/or indirect infringement by the Defendants of the '862 patent, including pre-judgment and post-judgment interest;

D. Increased damages as permitted under 35 U.S.C. §284;

E. A finding that this case is exceptional, and an award to Plaintiff SPA Syspatronic AG's of its attorneys' fees, expenses, and costs as provided by 35 U.S.C. § 285;

F. Judgment directing Defendants to pay costs and expenses in this action; and

G. Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38 and Loc. Civ. R. 38, Plaintiff SPA Syspatronic AG hereby respectfully demands a trial by jury as to all issues so triable.

Dated: September 18, 2007

By: O L Carroll

H. Michael Hartmann, *Lead Counsel*
Eley O. Thompson
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
Chicago, Illinois 60601-6731
Telephone: (312) 616-5600
Facsimile: (312) 616-5700

OF COUNSEL:
Otis W. Carroll
Texas State Bar No. 03895700
Wesley Hill
Texas State Bar No. 24032294
Ireland, Carroll & Kelley, P.C.
6101 South Broadway, Suite 500,
Tyler, TX 75703
Telephone: (903) 561-1600
Facsimile: (903) 581-1071

Attorneys for Plaintiff
SPA SYSPATRONIC AG

EXHIBIT A

US005093862A

United States Patent [19]

Scwartz

[11] Patent Number: 5,093,862

[45] Date of Patent: Mar. 3, 1992

[54] DATA CARRIER-CONTROLLED TERMINAL IN A DATA EXCHANGE SYSTEM

[75] Inventor: Hermann Scwartz, Pfäffikon, Switzerland

[73] Assignee: SPA Syspatronic AG, Zug, Switzerland

[21] Appl. No.: 381,510

[22] Filed: Jul. 18, 1989

[30] Foreign Application Priority Data

Jul. 20, 1988 [CH] Switzerland 02777/88

[51] Int. Cl.[5] H04L 9/32; G07F 7/08

[52] U.S. Cl. 380/25; 380/4; 380/21; 380/23; 380/50; 235/380; 235/382; 340/825.31; 340/825.34

[58] Field of Search ... 364/200 MS File, 900 MS File; 235/380; 380/2-4, 21, 23-25, 49, 50; 340/825.3-825.34

[56] References Cited

U.S. PATENT DOCUMENTS

3,925,710	12/1975	Ebert	317/100
4,450,535	5/1984	DePommery et al.	364/900
4,544,833	10/1985	Ugon	235/379
4,656,474	4/1987	Mollier et al.	380/23
4,672,182	6/1987	Hirokawa	380/25 X
4,683,550	7/1987	Jindrick et al.	364/900
4,683,553	7/1987	Mollier	380/4
4,786,790	11/1988	Kruse et al.	235/380
4,816,654	3/1989	Anderl et al.	235/380

FOREIGN PATENT DOCUMENTS

0111381	6/1984	European Pat. Off. .
0193920	9/1986	European Pat. Off. .

Primary Examiner—Bernarr E. Gregory

[57] ABSTRACT

A terminal (10) in a data exchange system with exchangeable portable user data carriers (4) has for their connection at least one connecting unit (3) and has further at least one data input unit (5). Exchangeable control modules (8, 9) are connected through one or more other, preferably similar, connecting units (6, 7). The modules are equipped with microprocessors and contain mechanically and cryptographically protected memory areas which receive secret data and keys for the secure carrying out of identity and authenticity tests, as well as application specific operational programs. These construction methods offer high security against unauthorized data access as well as against fraudulent manipulation of the device. They also greatly simplify the application independent design and construction of the terminal.

10 Claims, 2 Drawing Sheets

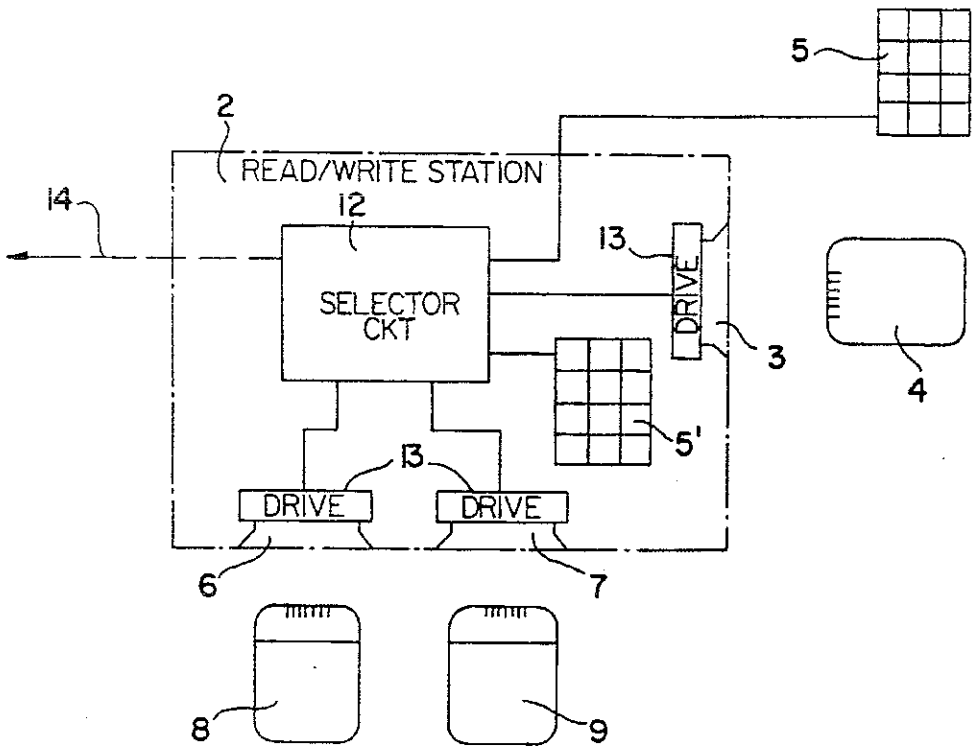


FIG. 1

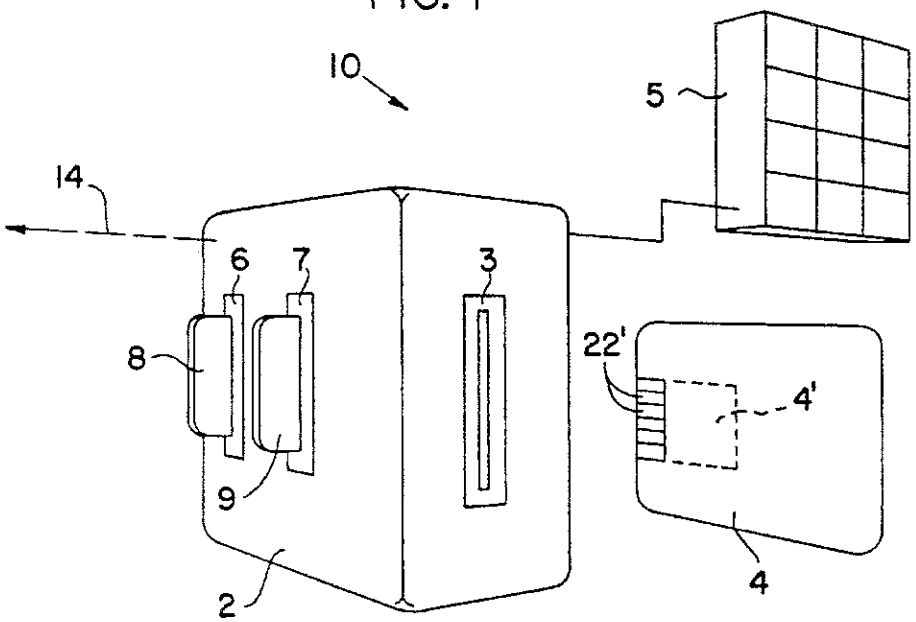

10
5
14
6
7
3
8
22'
4'
9
4
2

FIG. 2

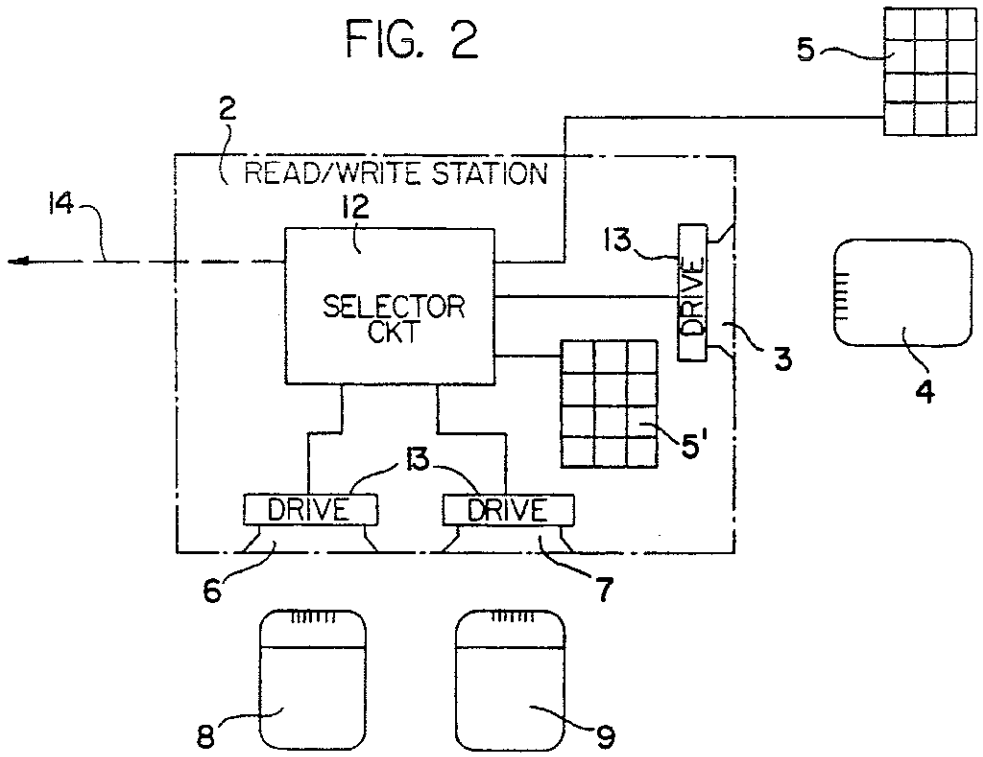
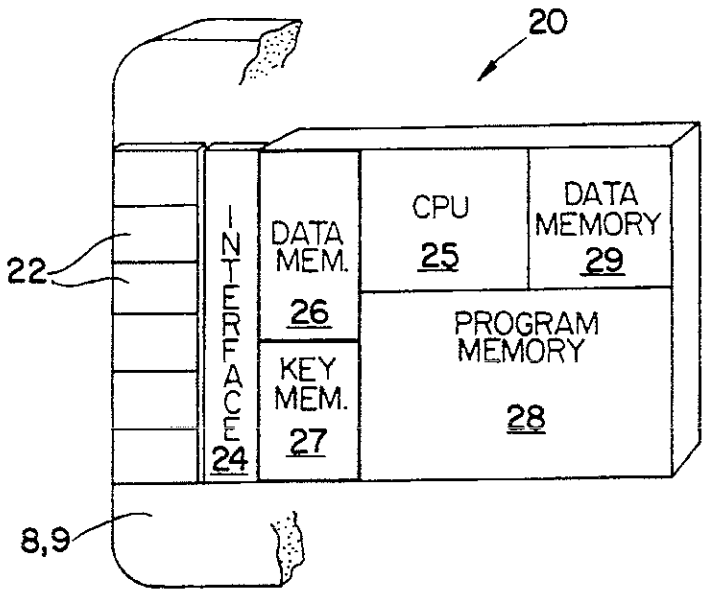

5
2
READ/WRITE STATION
14
12
13
SELECTOR CKT
DRIVE
3
4
5'
13
DRIVE
DRIVE
6
7
8
9

FIG. 3


20
22
INTERFACE 24
DATA MEM. 26
KEY MEM. 27
CPU 25
DATA MEMORY 29
PROGRAM MEMORY 28
8,9

DATA CARRIER-CONTROLLED TERMINAL IN A DATA EXCHANGE SYSTEM

BACKGROUND OF THE INVENTION

The invention concerns a data exchange system terminal controlled by portable data carriers, the terminal having several connection units for the connection of exchangeable user data carriers as well as other exchangeable data carriers, and also having at least one data input unit and a circuit means for assuring the performance of identity and authenticity tests.

Data exchange systems with terminals of this type are in constant development to achieve ever more numerous and more versatile uses. Above all, systems with user data carriers in the form of cards with built-in active, integrated semi-conductor circuits (so called chip cards) make possible ever more complex uses in expanded data networks, so that in most cases the trustworthiness and the secrecy of the data transmission takes on preeminent importance. To achieve a reduction in the transmission of large amounts of data (perhaps over large distances), there is a strong tendency to decentralize, that is to relocate data processing functions from central computers of the system to local terminals (generally existing in multiple numbers).

This requires, however, correspondingly more expensive and costly terminals, and to a similar extent also increases the risk of undesired manipulation and unauthorized access to secret data through the terminals. In this respect certain circuit parts are critical, these being those which undertake the testing of identity (authorization of a user to use a given data carrier) and of authenticity (that is the "genuiness" of a data carrier belonging to the system), because such decentralized testing presupposes the storage of secret test keys in the terminals.

Terminals of the aforementioned type with several connecting units for the connection of exchangeable data carriers are, for example, known from U.S. Pat. No. 4,450,535, FIG. 1, or from U.S. Pat. No. 4,809,326. In these devices the circuit means for carrying out the identity and authenticity tests are fixed components of the devices, that is they are built into the terminal, and in them the specific operational program is also stored. For performing the mentioned test procedures the secret test keys and if necessary further secret data must be read out of the exchangeable data carrier and temporarily stored in the device. This therefore results in an expensive and not very flexible construction of the device, and above all the devices are susceptible to unauthorized data access and fraudulent manipulation.

SUMMARY OF THE INVENTION

The present invention has therefore as its object the simplification of the design and construction of complex terminals for decentralized versatile use, and at the same time the decrease of critical security risk.

This object is solved in accordance with the invention by means of a terminal of the aforementioned type wherein the mentioned circuit means of the device are accommodated in at least one further exchangeable data carrier formed as a microprocessor containing control module and which, in connection with a control and computer means, is mechanically as well as cryptographically protected against unauthorized reading of the protected memory are which receives the secret test keys and other secret data as well as application specific

programs. This device and concept make possible a far reaching modular method of construction and with it a simple, cost-effective and application independent manufacture of multiple function terminals. Moreover the "modularization" implies high security against data access and manipulation at the device similar to that of microprocessor containing user cards, whereby the construction of largely automatic terminals—and correspondingly important saving in remote data transmission—is made possible without increased risk.

A number of preferred embodiments of terminals as well as accompanying control modules are possible.

BRIEF DESCRIPTION OF THE DRAWINGS

Further features of the invention appear in the following description of exemplary embodiments taken in connection with the drawings. The drawings show:

FIG. **1** a general view of an exemplary terminal embodying the invention,

FIG. **2** a simplified block diagram of the device of FIG. **1**, and

FIG. **3** a schematic illustration of an exemplary construction of a microprocessor in an exchangeable control module.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The terminal **10** of a data exchange system, such as illustrated in FIG. **1**, finds use for example as a so-called "point of sale" POS device or for example as an entrance control device or the like. The terminal **10** is controlled by portable exchangeable user data carriers **4**, here provided in the form of plug cards each having galvanized contacts **22'** and equipped with an active, integrated semiconducting circuit **4'** (so-called chip-cards with one or more semiconductor components). As a connection unit for the connection of the exchangeable user data carriers **4** a contact unit **3** is provided which, as illustrated, can be built into a read/-write station **2**. A data input unit to be operated by the user is illustrated as a key block **5** made separate from the station **2** and connected with it by a conductor. A further data input unit (not seen in FIG. **1**, illustrated in FIG. **2** at **5'**) can be provided for the operating personnel of the terminal (for example dealers, supervisors), just as customary alphanumeric indicating units for personnel and users can also be provided (not illustrated). External connections of the terminal to other units of the data exchange system, for example to a central computer, to other terminals etc., are illustrated at **14**.

The terminal **10** has two other connecting units, formed as contact units **6** & **7**, to each of which a control module **8** or **9**, respectively, is connected. These control modules are exchangeable and are equipped with one or more microprocessor whose construction and function is further explained below. In the case of the use of user data carriers **4** in the form of contact equipped plug cards it is of advantage if in the terminal similar contact units **3**, **6**, **7** and similar associated drive circuits **13** (FIG. **2**) are always used for the connection of the plug card **4** as well as for the connection of the control modules **8**, **9**. In this case all exchangeable control modules are also provided with a plug contact arrangement **22** (FIG. **3**) corresponding in size and in contact layout with that of the plug card **4**.

The individual exchangeable control modules available for the terminal **10** can be arranged in functionally special different groups according to the use assigned to the user data carriers. With reference to the arrangement at the device or to the exchangeability, different variations are possible according to application. Departing from FIG. **1**, (in addition to the contact unit **3** for the user data carrier **4**) only one single further contact unit can be provided by means of which different control modules can be interchangeably connected according to use. On the other hand, in case of a number of contact units **6**, **7** several control modules **8**, **9**, as illustrated, can be connected simultaneously. A single available control module o several simultaneously connected control modules can be individually activated either by the manual input of data (at the unit **5** or **5'**) or automatically on the basis of identification data stored in the then connected user data carrier **4**.

The individual functional units of the terminal **10** can naturally be arranged in different ways. Departing from FIG. **1**, the contact unit **3**, the data input unit **5** and if need be a display unit can be arranged in a "user console" separate from the other units of the device. According to need other contact units, for example for different types of user data carriers, can be provided. In case of a POS terminal at least one data input unit and one display unit are preferably arranged together in a "dealer" operating unit further connected to a known type of electrical data cash register (for payment). It may further be practical to arrange the control modules with their contact units spatially separate from the other functional units of the terminal.

An exemplary circuit construction of a terminal—related to the example of FIG. **1**—is schematically illustrated in FIG. **2**. The station **2** contains essentially a selector or commutator circuit **12**, to which external connection conductors **14** as well as all functional units, such as data input units **5**, **5'** and drive circuits **13** for the contact units **3** or **6** and **7**, of the terminal are connected. The selector circuit **12** forms essentially only the connection between the named functional units and the external system components. All circuit parts relevant to security, especially for the carrying out of identity and authenticity tests, as well as specific circuits and programs for the different data carrier types (for example card groups) are on the other hand housed in the microprocessors of the exchangeable control modules **8**, **9** etc. Especially, the secret test keys for the mentioned tests are stored only in these control modules.

A possible construction of the microprocessor of a control module is schematically illustrated in FIG. **3** (the integrated semiconductor circuit is preferably but not necessarily arranged on a single chip). Connected to the contact arrangement **22** is an interface area **24** for the cryptographically secured exchange of data, whereby a special (additional) computer means can be provided for carrying out the highly developed cryptographic method inside of the processor. The actual control and computer means of the microprocessor is illustrated by the area **25**. The control and computer means (CPU) **25** are associated with different memory areas **26** to **29**. Included in these is an area **26** for storing data to be maintained in secrecy and an area **27** for storing cryptographic test keys (identity and authenticity tests) especially cryptographically protected with respect to access. For other data which are not to be especially protected a memory area **29** is provided, and in the area **28** are stored operational programs for the data and command exchange, which are specific to the immediate application (system application, type of terminal, type of user data carrier, etc).

Every communication over the circuit **12** (FIG. **2**) from and to the control modules **8**, **9**—in the case of chip cards also from and to the user data carriers **4**—is protected by cryptographic methods (symmetric and-/or asymmetric cryptographic methods such as for example DES, data encryption standards, RSA-method, etc.). The use of these cryptographic methods in the case of coding and decoding, authorizing, authenticating as well as forming and testing electronic characters (such as for example "message authentication codes", "authentication identifier", "FAC File Authentication") takes place inside of the control module and if applicable inside the chip card. The secret keys required for this are only in existence in their protected memory areas. They are used exclusively inside of the control module and are not read out into the station **2**. The same goes for the specific operational programs, that is the programs that actively control the entire test procedure, the data exchange operations, etc. Finally the protocol and/or updating processes in respect to the procedures carried out by means of the terminal can take place inside of the control module in memory areas provided therefor.

The use of a main key or keys derived therefrom in a control module, which keys are respectively specific to a designated group or to a certain type of user data card, makes possible the automatic identification and activation of a given control module as soon as a data carrier **4** of the involved type comes into play. On the other hand a module can also he activated by means of manual data input, for example by an operator of the unit **5'** of the terminal. It can especially be provided that a certain control module is so secured against unauthorized use that its activation is only possible by the input of a secret code (for example PIN).

An especially advantageous and additional security is naturally obtained in that during the time periods in which the terminal is not activated and remains unsupervised the control module can be taken away and kept in a secure place, for example in a safe, which naturally cannot be done with the entire device. In the control module the integrated semiconductor components are moreover embedded and protected mechanically, chemically and physically (with same techniques known in connection with chip cards)—the that is an unauthorized attempt to free a component of the module (for example of a stolen control module) leads without fail to the disability or destruction or loss of the secret data.

On the other hand the terminal is naturally not functional without an inserted control module. Since it contains no secret data or circuit parts for cryptographic operations and no memory for such data, keys or other information, an unpermitted access to the station **2** can at most influence the ability of the station **2** to function, but it does not bring security into question. The terminal for this reason therefore requires, when not being operated and when the control modules are removed and safely stored, no special attention or expensive security measures.

With the described modular construction in which all of the circuit parts and data relevant to security are contained in the control module an extremely high security against unauthorized access to secret data and

against fraudulent manipulation of the terminal is achieved. Moreover, the device can be assembled practically exclusively from standard components independently of the intended use whereby its manufacture is substantially simplified and reduced in cost. It is finally to be noted that the described construction methods are naturally not only usable in connection with chip cards, but also with other types of user data carriers, such as magnetic strip cards, optical cards, etc. or data carriers with combined memory techniques (so-called hybrid cards). Instead of connecting units (for the cards as well as for the module connection) with galvanized contacts other types of connecting techniques can also be used (for example, inductive, capacitive, optical, etc.). In such cases under "contact arrangement" of the user data carriers (plug cards) or of the modules corresponding connection and transmission means are to be understood.

I claim:

1. A terminal (**10**) in a data exchange system controlled by portable data carriers, the terminal having several connecting units for connection of exchangeable user data carriers (**4**) as well as other exchangeable data carriers, at least one data input unit (**5**) and circuit means for carrying out identity and authenticity tests, further characterized in that the mentioned circuit means of the terminal (**10**) is housed in at least one of the other exchangeable data carriers different from the exchangeable user data carriers and is formed as a control module, the circuitry means so housed including a control and computer means (**25**) as well as memory areas (**26, 27, 28**) mechanically and cryptographically protected against unauthorized reading for storing secret test keys and other secret data, as well as application specific operational programs for the terminal.

2. A terminal according to claim **1** further characterized in that one connection unit is provided for the selective connection of any one of a plurality of different control modules at a time.

3. A terminal according to claim **2** further characterized in that the circuit means so housed further includes means for individually activating the control modules from manual data input or identifying data stored in user data carriers (**4**).

4. A terminal according to claim **1** further characterized in that several connecting units are provided for the connection of each one of the control modules.

5. A terminal according to claim **1** further characterized in that the user data carriers are plug cards (**4**) equipped with an integrated semi-conducting circuit (**4'**).

6. A terminal according to claim **5** further characterized in that the connecting units and associated drive circuits (**13**) for the user data carriers and (**4**) for the data carrier housing said circuit means forming the control module (**8, 9**) are similar.

7. A terminal in a data exchange system as defined in claim **1** wherein a circuit within the terminal has a cryptographic communication link with at least one of the exchangeable data carriers.

8. A terminal in a data exchange system as defined in claim **1** wherein secret test keys required for the cryptographic communication link between the circuit within the terminal and said one of the exchangeable data carriers are used and reside only within said one of the exchangeable data carriers.

9. A control module for a terminal (**10**) in a data exchange system, the terminal having a first connecting unit (**3**) for at least one portable user data carrier and a second connecting unit, for another portable data carrier comprising:

a portable data carrier removable from and insertable in the second connecting unit and having circuit means housed therein for controlling the terminal, the circuit means including control and computer means (**25**) and memory areas mechanically and cryptographically protected against unauthorized reading for storing secret test keys and other secret data as well as an operational program which is application specific to the terminal.

10. A control module according to claim **9** for a terminal (**10**) controlled by a portable user data carrier (**4**) having a plug contact received by the first connecting unit, further characterized in that the data carrier which comprises the control module has a plug contact arrangement (**22**) which in size and layout corresponds to that (**22'**) of the user data carriers (**4**).

* * * * *